Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
	)	
Digital Broadcast Content Protection	)	MB Docket 02-230

COMMENTS OF
DIGITAL TRANSMISSION LICENSING ADMINISTRATOR, LLC TO
FURTHER NOTICE OF PROPOSED RULEMAKING

The Digital Transmission Licensing Administrator LLC ("DTLA") is pleased to submit these comments in response to the Further Notice of Proposed Rulemaking ("FNPRM") in the Report and Order issued in above-captioned proceeding, dated November 4, 2003 ("R&O"). DTLA applauds the Commission for its continuing efforts to create a balanced protection regime that addresses the legitimate interests of all participants, namely:

- Content owners' concerns against the unfettered unauthorized redistribution of digital terrestrial broadcast content
- Manufacturers of consumer electronics and information technology companies' interest in developing and marketing innovative products at reasonable prices, and
- The paramount right of consumers to use and enjoy both broadcast programming and digital networking and recording technologies, consistent with reasonable and customary personal use practices.

DTLA is the licensor of the Digital Transmission Content Protection technology ("DTCP") that can be used to protect against unauthorized redistribution of digital commercial entertainment content, including digital terrestrial broadcast television. DTLA has licensed DTCP to more than 75 companies, including consumer electronics manufacturers, semiconductor manufacturers, information technology companies, major motion picture studios, and cable and satellite video services. DTCP can be used to protect commercial audiovisual and audio entertainment content over high-speed bidirectional digital interfaces, and is currently mapped for use over Internet Protocol (including 802.11 and wired and wireless Ethernet), IEEE 1394, USB and MOST interfaces. Additional information concerning DTCP, including informational versions of the Specifications, license agreements and policy statements, are available for review and downloading from the DTLA website, http://www.dtcp.com

The companies that developed DTCP – Intel Corporation, Hitachi, Ltd., Matsushita Electric Industrial Co., Ltd., Sony Corporation and Toshiba Corporation (collectively, the "5C Companies") – actively participated in inter-industry discussions concerning the technical implementation of the rc_descriptor in the ATSC A/65 standard as a "broadcast flag." DTLA

filed comments in this proceeding pursuant to the Notice of Proposed Rulemaking published by the Commission, *Digital Broadcast Copy Protection*, 17 FCC Rcd 16027 (2002) ("*NPRM*").

DTLA responds below to the questions posed by the Commission in the numbered paragraphs of the FNPRM. The majority of DTLA's comments address the Commission's consideration of the potential utility of functional criteria to describe certain attributes of a technology that protects Unscreened Content and Marked Content[1] across digital networks. DTLA suggests, in Appendix A, certain functional criteria for consideration by the Commission. Notwithstanding, DTLA candidly believes that even its own technology-based functional criteria, by themselves, do not measure all of the complex considerations that determine acceptability of a particular protection technology. A technology that may not satisfy every functional criterion may offer overall a more protective method than a particular technology that meets each of the criteria. For example, a content protection means that requires only modest robustness but is supported by strong patent position and a dedicated enforcement plan could provide ample protection for content owners. Similarly, a technology that falls just shy of one functional criterion but exceeds all other minimum functional requirements may, in the aggregate, provide sufficient protection.

Therefore, DTLA strongly urges that use of functional criteria by the Commission for certification of protection technologies should be *an additional alternative to, and not in lieu of*, use of the market-based Joint Proposed Criteria previously submitted by DTLA along with its December 6, 2002, comments in this proceeding. Those criteria are attached hereto for convenience at Appendix B.

Response to Commission Questions in the FNPRM

I. DTLA Does Not Support Encryption of the Basic Service Tier as a Means to Signal Redistribution Control.

Paragraph 59. Whether cable operators that retransmit DTV broadcasts may encrypt the digital basic tier in order to convey the presence of the ATSC flag through their conditional access system. Section 76.630 of the Commission's rules generally prohibits cable operators from "scrambl[ing] or encrypt[ing] signals carried on the basic service tier" without distinguishing between analog and digital service. NCTA has suggested that allowing cable operators to encrypt the digital basic tier and "virtually" convey the presence of the flag will facilitate the offering of future home networking services. We seek comment on whether cable operators should be allowed to encrypt in this manner.

As a general principle, the 5C companies recognize that applying protection (such as encryption) at the source provides better and more appropriate protection than attempting to re-protect content delivered in the clear. In this circumstance, however, the Commission justifiably concluded, in Section III.B of the R&O, that implementation costs, delays, and the burdens imposed upon consumers by forced obsolescence of legacy equipment, make source encryption a

[1] Capitalized terms have the meaning set forth in the Commission's Regulations at 47 C.F.R. § 73.9000 "Definitions."

less palatable solution for addressing the problem of unauthorized redistribution than the broadcast flag.

Encryption of a cable signal serves different purposes from that of the broadcast flag. Encryption of cable signals typically is intended to protect the commercial interests of the system operator, *i.e.*, to control access to the encrypted signals only to paid subscribers, and thereby secure the revenue stream of the system operator. That commercial interest exists regardless of whether the content being delivered by the system operator is Marked Content. The broadcast flag, by contrast, is intended to protect the interests of the content owner. This distinction is important insofar as not all broadcast content in the basic tier may be marked with a broadcast flag. Indeed, a content owner could have legitimate reasons to prefer not to assert redistribution control, *e.g.*, to build an audience for a new program by word of mouth or to enable more people to watch programming at a time and place of their convenience.[2] Moreover, it is desirable that certain content – such as Presidential addresses, Congressional sessions, and other events of public importance – not be delivered in any form that hinders free redistribution. Hence, the choice *not* to mark content against redistribution promotes the interests of the public and the content owner and should be respected. If encryption of the digital basic service tier automatically would trigger redistribution control, the rights of the public and the preferences of content owners unfairly would be trumped by the commercial interests of the cable operators.

While the public interest *could* be accommodated by permitting encryption *only* of Marked Content, the risks of erroneous encryption and consumer confusion outweigh any benefit to the cable companies of not using a separate flag mechanism. The 5C companies therefore submit that cable (and satellite) operators thus should maintain independent means of signaling the presence of the broadcast flag, and should not be permitted to use the fact that content is encrypted to signal that redistribution control is to be applied.

II. DTLA Supports Adoption of Standards and Procedures for Certifying Protection Technologies.

Paragraph 61. Whether standards and procedures should be adopted for the approval of new content protection and recording technologies to be used with device outputs on Demodulator Products. If so, we seek comment on the various types of content protection technologies that should be considered as a part of this process, including but not limited to digital rights management, wireless and encryption-based technologies. We recognize that similar issues have been raised with respect to digital cable ready DTV receivers in the Second Further Notice of Proposed Rulemaking in the Commission's ongoing "Plug and Play" proceeding. We seek comment on whether a unified regime should be employed in both instances.

DTLA supports adoption of standards and procedures that would facilitate the rapid approval of any technology that demonstrably can provide effective protection against unauthorized redistribution of digital terrestrial broadcast content. Adoption of standards and

---

[2] *See Sony Corporation of America et al. v. Universal City Studios, Inc.,* 464 U.S. 417, 443-447 (1984).

procedures can assure that protection technologies will satisfy requirements of protecting content and will give guidance to technology vendors and product manufacturers. Such standards will ensure a regime that correctly balances the interests of all parties, including the public interest, and will reduce the potential for protracted disputes and lawsuits as to whether particular technologies provide adequate protection.

DTLA believes there should be no limitation as to the type of the technologies that may be certified through this process, so long as such technologies provide effective protection against unauthorized re-distribution. There are several mature known security and rights management systems in use today that rely on scrambling or encryption, but new alternative technologies may produce effective protection systems in the future. Predetermining the nature of effective technologies or otherwise limiting in any artificial way the types of technologies that might be used for redistribution control could stifle competition and innovation.

Therefore, DTLA submits that any standards and procedures adopted by the Commission should observe the following general principles:

- The Commission should neither preclude nor require the use of particular technologies. Rather, the Commission's standards and procedures should facilitate approval of any technological method that provides reasonable protection against unauthorized redistribution of Unscreened Content and Marked Content.

- The Commission's standards should permit interoperability between and among consumer electronics devices and information technology products, but should not require that all systems must be interoperable. Effective technologies should be permitted to be applied even to closed systems that work only with a particular type or brand of product.

- Standards and procedures should not restrict the potential application of technologies to particular networking platforms (*e.g.,* wired or wireless) so long as the technologies provide sufficient protection on each platform on which they may be implemented.

A. The Commission Should Adopt Alternatives of Both Market-Based Criteria and Additional Functional Criteria.

Past submissions of the DTLA in this proceeding supported adoption of "Joint Proposed Criteria," in conjunction with MPAA companies. In brief, these are:

(1) 3 Major Studios and/or Major Television Broadcast Groups (of which at least 2 must be Major Studios) use or approve the technology;

(2) 10 Major Device Manufacturers (including software vendors) have licensed the technology and 2 Major Studios use or approve the technology;

(3) The technology is at least as effective at protecting Unscreened Content and Marked Content against unauthorized redistribution as is any other technology then certified pursuant to the Commission's standards and procedures; and,

(4) The technology (together with its license terms) includes output and recording control that protect against unauthorized redistribution of audiovisual content, and such technology was expressly named as being permitted to be used for the output or recording (as applicable) of audiovisual content under license applicable to a technology either (a) at the time such technology is approved by FCC, or (b) at a later date, provided that a Change Management process applied to such subsequent approval.

See "Joint Proposal from MPAA and 5C Companies," December 6. 2002, attached to Comments of MPAA et al. and Comments of DTLA, and attached hereto at Appendix B.

Inasmuch as content owners are the parties most concerned with protecting against unauthorized redistribution of broadcast programming, there is no logical reason not to certify any technology that is acceptable to content owners (*i.e.,* that has been "used or approved" by content owners, per the 5C-MPAA Joint Criteria Proposal under Criteria (1), (2) and (4)) -- ***so long as the Commission provides additional alternative means by which any proponent can obtain prompt and independent certification of its technology, without the requirement of use or approval by any other stakeholder.*** Criterion (3) provides one such alternative method, and DTLA continues to strongly support the adoption of that criterion, and all four of the proposed market-based criteria, as appropriate and necessary criteria for certification of acceptable protection technologies. (An additional method, as the Commission suggests, would be by satisfying functional criteria, which will be discussed below.)

Separately, if a certified protection technology subsequently authorizes Broadcast Flag content to be protected by another downstream technology, then logically the Commission also should certify such additional downstream technology. Criterion (4) above suggests two alternative methods by which such authorization could occur, that is, by Commission approval or by subsequent use or approval of content owners pursuant to "change management" provisions in any license to the technology. In such circumstance, the end result of the protection where a Demodulator Product directly passes digital terrestrial broadcast content to such downstream technology is no different from when such content is input to such technology via an intermediate Commission-certified technology.

DTLA also supports the concept of functional criteria as an additional means to attain approval. In response below to paragraph 62 of the FNPRM, DTLA discusses the pros and cons of many of the specific criteria that were referenced by the Commission in the FNPRM. At Appendix A to these Comments, DTLA proposes alternatives and modifications to these functional criteria suggestions that, DTLA respectfully submits, might serve as the basis for further discussion from commenting parties. DTLA urges the Commission to adopt both the Joint Proposed Criteria and functional criteria, each as alternative and independent means to obtain certification, so as to establish multiple processes by which as many secure technologies as possible may be authorized for use by product manufacturers.

B. Digital Output and Recording Protection Technologies Certified for Use in Either the DFAST License or PHILA Should Automatically be Approved to Protect Unscreened and Marked Content.

Concerning the last question addressed in paragraph 61, the 5C Companies believe that it may not be appropriate to adopt the same criteria for certifying technologies that can protect against redistribution in both the Plug and Play and Broadcast Flag proceedings. Digital terrestrial broadcast programming is among the content to be protected by digital cable and satellite navigation devices addressed in the Plug and Play proceeding. However, cable and satellite services also may deliver to consumers additional content that, traditionally, has been released by certain content owners in earlier delivery windows and that potentially may have a higher economic value (such as motion pictures, programming and live events delivered by video on demand or pay subscription channels). Protections for such programming extend beyond the concerns of redistribution control, and encompass also Encoding Rules that may apply more stringent copy control encoding (e.g., "Copy Never" or "Copy One Generation") to non-broadcast delivery methods. [3]

Because the programming that is the subject of this proceeding clearly is also protected by technologies approved for use on cable and satellite services, any digital output protection technology or digital recording technology approved for use either in the DFAST license or in the PHILA should automatically be approved for use as a redistribution control technology for purposes of this proceeding.[4] Such a result would provide significant benefits. First, it would reduce administrative burdens upon the Commission to perform unnecessary and redundant technology certification procedures, when a single appropriately-stringent analysis could readily accomplish both purposes. Second, such a proposal would result in cost savings for manufacturers who already will be designing and deploying such technologies into receivers, displays and recording devices. A manufacturer would not need to implement separate protection systems, which would prove expensive and cumbersome to design and manufacture. Similarly, a manufacturer would not need to delay implementation of a particular technology for Plug and Play purposes pending approval of a technology for protecting redistribution of only broadcast content. Third, permitting more rapid approval of broadcast protection technologies will promote the interests of content owners and the Commission in attaining a timely rollout of redistribution controls for digital broadcast television programming. Finally, such a procedure would facilitate ease of consumer use and interoperability among home digital television equipment by ensuring that the same protected digital output connections can be used for both programming delivered only via cable or satellite and via digital terrestrial broadcast transmission.

---

[3] For that reason, the lack of approval of a particular technology for use under the DFAST license or the PHILA should not affect the Commission's decision as to the acceptability of the technology for redistribution control of digital broadcast television.

[4] This position appears to also be supported by the MPAA companies, as set forth in their *ex parte* filings with the Commission dated October 28 and 31, 2003.

III. DTLA Supports the Adoption of Appropriate Functional Criteria as an Additional Means of Certification.

62. Whether objective criteria should be used to evaluate new content protection and recording technologies and, if so, what specific criteria should be used. For example, in our recent Second Report and Order and Second Further Notice of Proposed Rulemaking relating to digital cable compatibility, Microsoft Corporation and Hewlett Packard Corporation submitted a detailed proposal suggesting functional requirements that could be used to evaluate digital rights management technologies for use with digital cable ready products. We seek comment on this proposal in the ATSC flag context, as well as on other proposals submitted in this proceeding relying on objective criteria, and any new proposals that commenters may submit to the Commission.

DTLA in its Comments and ex parte submissions to the Commission in this proceeding consistently has supported the concept of "functional criteria." We observed that any criteria must:

-- establish with specificity the minimum level of protection to be required of any technology, yet

-- retain enough flexibility for approval of alternative future protection methods so as not to stifle or hinder innovation.

Unquestionably, functional criteria can provide an important additional means to obtain certification. Notwithstanding, the 5C Companies believe that functional criteria cannot capture all of the complex factors that are considered in any determination as to whether a particular technology, considering its technical attributes, marketing characteristics and enforcement means, can provide adequate protection for broadcast content. Consequently, reliance on functional criteria as the sole means of obtaining certification could result in the unnecessary and unwarranted exclusion of protection technologies that otherwise would provide an acceptable level of protection. Therefore, DTLA submits that functional criteria should supplement (as a separate and alternative path to approval), but not substitute for, the market-based Joint Proposed Criteria.

The Commission, in its R&O, referred to certain criteria that had been suggested in comments or ex parte presentations by four groups: Hewlett-Packard and Microsoft; Philips; Dell and the IT Coalition. *See* R&O at 25, n. 141 and 142. DTLA believes that several of the functional criteria put forward in some of those proposals, and particularly the comments of Dell, reflect a productive and useful starting point for further consideration. DTLA further anticipates that these and other participants to this proceeding have continued to consider these issues, and therefore looks forward to reading their comments in this FNPRM proceeding.

In particular, DTLA agrees that many of the broad categories for criteria (*i.e.,* Scope, Security, Strength, Robustness, and Revocation) are appropriate subject matter for functional criteria. We regard a number of other proposed criteria, however, as unnecessarily restrictive, unrelated to security considerations relevant to redistribution control of broadcast content or flawed in ways that render them unsuited to criteria for a broad range of products and technologies.

Accordingly, DTLA comments below on several of the above-referenced proposals, focusing in section A below on those elements of the October 24, 2003 submission from Dell, Inc that are generally supported by DTLA, and offering suggestions as to the specific text of such criteria; reviewing in section B two attributes that merit consideration, although should not be adopted as functional criteria, *per se*; and, discussing in section C the reasons why certain other criteria referenced by the above-referenced commenters should not be included in any standards and procedures adopted by the Commission.

A. Functional Criteria Supported by DTLA

DTLA sets forth below its proposed functional criteria for use in determining whether particular digital output and recording protection technologies should be certified by the Commission under § 73.9008. The adoption by the Commission of these criteria should not impose any requirements on Demodulator Products or other products that implement or use technologies approved under these criteria.

1. Scope of Redistribution

DTLA agrees that it may be useful to define a criterion for "Scope." The Dell "Scope" proposal stated:

> "The content protection method must prevent the unauthorized redistribution of digital television broadcasts to the public when such an interest in securing protection is signaled by use of a broadcast flag."

No protection system can "prevent" unauthorized redistribution as an absolute requirement. Hacking of any system is virtually inevitable, and many secure systems define the boundaries of "legitimate" and "illegitimate" distribution with sufficient (but not absolute) precision. A technology should not be disqualified simply because it may be possible to hack the technology or to use the technology outside the ordinary course of operation (*e.g.,* where someone intentionally passes a wire through to a neighbor's apartment or gives a password to a neighbor). Rather, it should be sufficient that the technology be designed to restrict unauthorized redistribution in the ordinary course of its operation.

Inasmuch as the Scope applies to both digital output protection technologies and digital recording protection technologies, DTLA proposes also to clarify, consistent with Encoding Rules applicable to protected digital broadcast content, that protected copies can be copied and distributed on physical media, although not by electronic redistribution.

Therefore, the 5C Companies suggest revising the Dell proposal on Scope as follows:

> "The content protection method must be capable in the ordinary course of its operation of reasonably restricting the unauthorized redistribution outside of the home and personal digital network of Unscreened Content or Marked Content. For clarification, the content protection method need not impose any restrictions with respect to the distribution or playback of physical copies of Unscreened Content or Marked Content."

2. Security Method

DTLA recognizes that while DTCP and other content protection technologies rely on encryption and key authentication as essential elements of security, the Commission should not preclude other, equally protective mechanisms, that may be developed. Therefore, DTLA proposes to define a criterion describing the essential elements of a "Security Method," as follows:

"The content protection method must include either—

(a) an authentication, content encryption or scrambling, and key management process that is designed to ensure that Unscreened Content or Marked Content cannot be accessed in usable form except by a device that has appropriate credentials (*e.g.,* keys), or

(b) an alternative mechanism offering at least an equivalent level of protection."

3. Robustness

"Robustness" generally reflects the resistance of the implementation of the technology to efforts to defeat the protection measures. DTLA notes that MPAA has filed a Petition for Reconsideration with the Commission with respect to the Robustness Requirements. Ultimately, any robustness requirements applicable to a given protection technology should establish the same minimum degree of protection as required by Section 73.9007, so as to provide reasonable protection against unauthorized interception of content or circumvention of the content protection requirements identified in the scope criteria. Thus, the criteria could simply state:

> "The content protection method must provide for or require implementation with at least the level of robustness required under § 73.9007 for a Covered Demodulator Product."

4. Data on a User Accessible Bus

DTLA proposes that a "user accessible bus" standard should reflect the same requirement set forth in the Commission's regulations at 73.9006, so as to prevent the availability of clear compressed video data on a user accessible bus as follows:

> "The content protection method must restrict Unscreened Content or Marked Content from being passed in unencrypted compressed form via a User Accessible Bus at least to the same extent as is required by § 73.9006."

5. Strength

The "Strength" criterion exemplifies some of the difficulties inherent in setting generic rules for developing technologies. Strength of a particular technology is measured according to the technology's attributes; some easily measured, *e.g.*, the length of an encryption key and others less easily measured, *e.g.,* resistance of a cryptographic algorithm to cryptanalysis. However, describing Strength only in terms of known technologies could unintentionally limit the possible technologies that might be applied for protecting Unscreened and Marked Content in

the future. The criterion proposed below attempts to balance the need to give specific guidance (*e.g.*, a "safe harbor" method of complying with the Strength requirements), and sufficient flexibility in approving non-cryptographic implementations that demonstrate comparable effectiveness.

Several of the comments, including the October 2003 *ex* parte submissions from the IT Coalition and Microsoft-Hewlett-Packard, proposed that an encryption algorithm must be a "public" standard technology. DTLA respectfully submits that this proposal is unnecessarily restrictive. Certainly, public standard algorithms, such as DES or AES, have demonstrated their trustworthiness in public testing. However, in many cases proprietary scrambling or cryptographic algorithms are employed for content protection (*e.g.,* proprietary encryption systems used by cable and satellite systems, as well as the M6 cipher used for protecting satellite delivery of video content in Japan and used as one baseline encryption method for certain implementations of DTCP). These proprietary algorithms are regarded as effective for protection of premium content. Therefore, use of both public standard and effective proprietary algorithms should be permitted under Commission regulations.

DTLA therefore suggests that the Strength criterion might be expressed as:

> "If the content protection method uses cryptographic algorithms to protect content against unauthorized redistribution, such cryptographic algorithms must use key length of at least 56 bits. The algorithm must be such that detailed knowledge of the algorithm shall not, in and of itself, be sufficient to enable circumvention. If the content protection method uses methods other than cryptography to protect against unauthorized redistribution, it must provide for at least an equivalent level of protection."

6. Authentication

DTLA proposes addressing Authentication as part of the criterion for "Security Method" (*see* Section III.A.2).

Several comments also cite "authentication" as a requirement, but suggest that devices that exchange content somehow must verify their *compliance* with the protection system or the regulations. This seems to ignore that authentication systems typically test only whether the two devices or systems each can provide *indicia* of compliance (such as knowledge of a shared secret) and not compliance itself. Indeed, source devices cannot authenticate whether the sink device is fully compliant (*e.g.,* has not been hacked) and vice versa, and should not be required to do so.

Moreover, some of the suggested criteria refer to specific known implementations, such as public key identification. While such systems are in common use today, DTLA submits that the regulations should not preclude or delay introduction of alternative technologies that may be under development now or in the future.

DTLA therefore suggests that the "Authentication" requirement should be only that a device must obtain some verification or technical assurance that it is passing or exchanging the content to a device that indicates, through some technological credential or indicia, that it is

authorized to implement the approved content protection method.[5] Any criterion should not be specific to any particular authentication method or technology.

7. Revocation

Initially, DTLA believes it would be helpful to clarify the intended terminology, inasmuch as "Revocation" has a particular meaning in many content protection agreements. The Commission also used the term "revocation" in paragraph 65 of the Report and Order in a manner that appears to be different from what is meant here.

In the Adopter and Content Participant Agreements for DTCP, "revocation" means the technical ability to revoke the credentials (*e.g.*, a device certificate) of a device, which results in the isolation of the revoked device such that other devices will refuse to exchange content protected with that technological method with the revoked device. DTLA has enabled the possibility of revocation as an extraordinary and drastic remedy. Revocation is to be applied only in circumstances in which the secret key associated with a device certificate has been lost, intercepted or stolen, or in which the certificate has been cloned and installed in multiple devices, or pursuant to order from a governmental authority. In accordance with the terms of the above-reference DTCP agreements, revocation is permitted only with the consent of the affected device manufacturer or upon an arbitrator's determination that these standards have been met. These revocation standards are applied to all types of content protected by DTCP. To date, DTCP Revocation has never been requested or used. DTLA notes that similar provisions regarding revocation have been adopted in conjunction with the Plug and Play proceedings, where revocation of device certificates provided under DFAST may occur only upon loss, cloning or governmental order.

DTLA therefore believes that revocation of a particular device should be required in this proceeding only in the above limited circumstances. Importantly, revocation should not be viewed or utilized as a response to instances in which a protection technology may be hacked or in which the devices are found to be non-compliant. In this sense, DTLA believes that the suggested rule in the October 2003 IT Coalition, Dell and Microsoft/Hewlett-Packard submissions that "revocation" should be required when a protection technology is compromised is unrealistically stringent. The possibility that products within the home might subsequently be revoked would have a severe impact on consumers and the transition to digital technology as a whole. Consumers may not understand why the product suddenly failed to function; and a user who has legitimately acquired and been using a product only for lawful purposes might justifiably bristle at revocation.

---

[5] DTLA also questions the IT Coalition suggestion that "Management of decryption keys must be controlled so that only specified persons may obtain access to the content." It is not clear whether this suggestion was intended to require a device to authenticate literally a particular person, or only to require authentication that a product is a licensed product. If the former was the intention, this could raise privacy concerns about the collection of personal identification information (as well as potentially requiring the implementation of a technologically highly complex mechanism).

Revocation therefore should be required, at most, for only those few exceptional cases where a secret key associated with a device certificate, or an equivalent device security identifier, becomes lost, stolen, or cloned, as follows:

> "If the content protection method relies on a secret key for protecting content exchanged between products, it must be technologically possible to revoke the ability of an individual product to access in usable form Marked Content or Unscreened Content if such key and/or an associated device certificate has been:
>
> (a) cloned without authorization of the entity generating or licensing the keys, or,
>
> (b) lost, stolen, intercepted or otherwise misdirected, or made public or disclosed in violation of a license agreement, if applicable."

DTLA discusses, *infra,* at Section III.C.2, the role of renewal or upgrading of protection technologies for particular types of protection systems. DTLA considers that the above "Revocation" criterion would be satisfied by, but would not require, renewal of a content protection method, inasmuch as the process of renewal or substitution of a given protection method that relies upon a secret key would render the original key unusable.

B. Additional Considerations

1. Change Management

As a general principle, owners of certified technologies should be free to make periodic updates to their technologies and, if applicable, licenses, so long as there are adequate protections that ensure that such changes will not materially and adversely affect the level of security applied to Unscreened and Marked Content. For licensed technologies, one way of ensuring that future changes will maintain such effective protection is to include in the license "change management" procedures whereby content owners have a right to review and oppose changes that may materially and adversely affect their rights under the license agreement. (The DTCP Content Participant Agreement includes change management provisions beginning at section 3.7.)

Where a technology has an agreement available to content owners that provides such a specified right or ability to meaningfully object to material and adverse changes, the Commission should deem that any changes made to the technology or licenses (if applicable) do not have a material or adverse effect on the level of security. Where a technology does not provide for change management rights for content owners, then such technology proponent should be able to certify to the Commission that any changes continue to satisfy the functional criteria adopted by the Commission or otherwise are consistent with the standards and procedures established by the Commission at the time the changes were made. Such certification could be pursuant to a simplified procedure that provides that material changes that affect the security or integrity of the technology should be subject to public notice and objection. DTLA submits that such procedures are far more streamlined than the criterion proposed by Philips, which would require that any changes to a protection technology or its license terms be subject to consensus among all licensees and content owners. At best, such a process would be highly impractical, time-consuming and unduly cumbersome, and would likely delay for many months the adoption of changes to a technology that are beneficial and/or necessary. DTLA also would be concerned that the Philips proposal would enable any competitor (indeed, companies that market competing

protection technologies) to stymie necessary or advantageous technology changes for anticompetitive purposes, while insulated by government regulations.

2. Proprietary Technology

DTLA supports the approach taken in the Commission's interim procedures that provides for the certification of both proprietary and licensed content protection technologies. *See* 47 C.F.R. § 73.9008(4); FCC Public Notice DA 04-145 at 2 (January 23, 2004). Accordingly, DTLA supports the adoption by the Commission of standards and criteria that permit the certification of, and apply equally to, both proprietary technologies and licensed technologies. There is no reason to disapprove an otherwise effective technology that a company wishes to market only in its own products. The Commission's interest should extend only to the level of protection offered by the technology, not the marketing strategy employed by the proprietor; the marketplace can decide whether such products will succeed. DTLA therefore disagrees with the Philips-proposed criterion to certify only technologies that may be licensed to others.

C. Additional Factors that are Not Appropriate Subject Matter for Functional Criteria

We agree with the comments of Dell that several additional considerations, although potentially relevant to a decision by a technology implementer whether to deploy one or another technology, should not be included in any functional criteria or other regulatory scheme. Many of these proposed criteria can be addressed by the marketplace evaluation of which technologies should be adopted for use in protecting Unscreened and Marked Content. Thus, as long as the Commission adopts standards and procedures that promote the certification of a multitude of technologies, competition will more than adequately address these additional factors, which are discussed below.

1. Rights

Several of the proposals include criteria relating to the inclusion of rights management information in the data stream. DTLA believes that rights-related criteria are not appropriate subject matter for criteria, for two reasons.

First, for purposes of approving technologies in the Broadcast Flag context, the only relevant inquiry with respect to "rights" is whether the technology restricts the content within the Scope. Redistribution control can be achieved in a number of ways that do not necessarily require the transmission of rights information. Some systems, such as HDCP, protect content as the last link in the chain; because HDCP-protected content is sent to a display and cannot be retransmitted thereafter, the protection itself is all that is needed and no additional rights information needs to be conveyed. A rule that requires the conveying of rights information would therefore unnecessarily disqualify potentially effective technologies.

Second, whether and how additional rights (beyond redistribution control) may be addressed by the technology is not relevant to the question of whether the technology protects Unscreened and Marked Content from unauthorized distribution.

The specific proposal to incorporate rights information based upon XrML technology is not necessary or appropriate in the context of this proceeding. XrML is beginning to become deployed in certain IT digital rights management ("DRM") systems, but is not commonly implemented in consumer electronics products and, hence, might prove inefficient and impractical for all products subject to this regulation. Further, XrML is designed to handle

complex usage rules in DRM systems that are far more capacious and elaborate than the simple "presence/absence" information that needs to be conveyed by the ATSC rc_descriptor. Thus, while functional criteria should not preclude the use of any DRM, which should be free to use XrML if desirable; there is no need for the criteria to specify or obligate use of XrML or any other right management standard.

For these reasons, any proposal regarding "Rights" is coextensive with and wholly duplicative of the Scope defined in the regulations. As such, there is no need for a separate Rights criterion, and we propose that the Commission need not adopt such a criterion.

2. Renewability and Upgradeability

Comments submitted in October 2003, by the IT Coalition and Microsoft and Hewlett-Packard proposed a possible criterion that a technology should be capable of renewal and upgrade. DTLA noted in its discussion of Revocation, *supra* at Section III.A.7, that renewability and upgradeability are possible means, among others, to respond to attacks or technological advances by renewal or upgrade. DTLA believes, however, that they are inappropriate as mandatory criteria. First, such a criterion is likely to be extremely exclusionary. Not every effective technology is inherently renewable, or can be upgraded without adversely affecting compatibility with prior devices in market. Consumer electronics products in particular generally are not readily renewable or upgradeable. CE devices typically implement content protection technology in non-upgradeable hardware, and are not typically connected to the Internet or other network that can download technology to renew or upgrade their content protection. Second, renewability potentially significantly increases cost of technologies (*e.g.,* by requiring replacement of smart cards), which costs ultimately are borne by consumers. Third, for the first two reasons articulated above, adoption of a renewal or upgrade criterion would inherently tilt the playing field against consumer electronics products, and in favor of software-based systems that may be renewed and upgraded with less burden and expense than CE hardware products. Finally, a requirement of renewal or upgrade is unnecessary. To date, no licensed technology generally applicable to consumer electronics entertainment products has mandated renewal or upgrade functions. Moreover, DTLA notes that even systems that have been hacked or otherwise compromised may still provide sufficient protection. As an example, CSS was "compromised" several years ago, and is not renewable or susceptible to a large-scale upgrade. Yet, despite the availability of circumvention tools, CSS remains extremely effective for its purpose of protecting high-value DVD content and "keeping honest people honest." Renewability and upgradeability clearly are not necessary to the effectiveness of a protection system. For the foregoing reasons, the DTLA strongly opposes adoption of criteria mandating renewability or upgradeability.

3. Interoperability

Interoperability, the ability of devices of different types and of different platforms to exchange information and work together, similarly is a generally desirable attribute. However, DTLA does not agree with the IT Coalition and Microsoft/Hewlett-Packard proposal that interoperability should be an absolute requirement. There may be technologies that offer effective protection, yet inherently are limited to particular platforms. One example is D-VHS, which is limited in its operation to certain digital videocassette recorders. In addition, it may be that particular technologies are inherently incompatible with one another, yet each is completely effective in protecting against unauthorized redistribution of Unscreened and Marked Content.[6]

---

[6] The IT Coalition proposal on interoperability suggests that "components of the system shall be interoperable and consistent with appropriate related industry standards." DTLA (continued…)

Manufacturers recognize, in accordance with the economic principle of network effects and Metcalfe's Law, that interoperability inherently increases the value of both interoperable technologies. DTLA therefore believes that sufficient economic incentives exist so as to promote interoperability, such that decisions with respect to interoperability of technological measures should best be left to the marketplace.

4. Performance, and Ease or Cost of Implementation

Microsoft/Hewlett-Packard proposed a criterion that requires protection systems to maintain a certain level of performance. Performance factors, including the computational burden placed by protection systems upon devices, are relevant to the decision of a company to implement one technology over another. However, performance has little to do with the effectiveness of the system, and so should not be a criterion for approval. For example, a technology that is more expensive to implement but carries a very low royalty could be more attractive in the market than a technology that carries a higher royalty but lower computational burden.

Similarly, although low cost and/or easy implementation of the technology are desirable, these need not be mandatory criteria for approving a protection technology. So long as the Commission adopts criteria that will enable certification of a large number of effective technologies, any manufacturer can choose a technology that strikes an appropriate balance of costs and efficiency. If the approved technology is too costly or requires complex implementation, a manufacturer can always adopt an alternative technology.

Thus, performance, cost or ease of implementation criteria are not necessary.

5. Implementation in Hardware and Software

The IT Coalition, Dell and Microsoft/Hewlett-Packard included in their proposed criteria that both software and hardware implementations of a technology should be allowed. DTLA again believes that such decisions are best left to the marketplace. It should not be a mandatory requirement that each protection license always must allow implementation of its technology in both hardware and software. For example, in some cases, a licensor might wish to license a technology only for hardware implementation, when the technology is largely dependent on physical characteristics for its robustness. Conversely, certain technologies may be optimized for software implementations, and could be largely unsuitable for hardware implementation. Again, so long as the Commission criteria do not bestow an inherent advantage upon hardware or software implementations, a technology proponent whose technology is readily adaptable to both hardware and software will have economic incentives to take advantage of the opportunity to license both hardware and software implementations, and so a mandatory criterion is inappropriate and unnecessary.

6. Avoiding Consumer Confusion

Microsoft/Hewlett-Packard proposed a criterion which requires avoiding consumer confusion, but this criterion, again, is unnecessary. It is in the manufacturer's best interest that

---

believes this proposal is potentially vague in that it provides no definition of what is an "industry standard"; and, to the extent that a standard in this field is attained via approval by the Commission, the proposal seems circular.

content protection methods do not cause user confusion. Thus, manufacturers will take positive measures to avoid problems such as not implementing approved technologies that the manufacturer believes will result in consumer confusion, even if the Commission does not require it.

7. Approval of Downstream Technologies

DTLA does not agree with the proposal by Philips that any Commission-approved technology shall be automatically deemed approved as an downstream output or recording protection technology by all other approved technologies. Of course, interoperability among protection systems can be a desirable feature and, under the economic law of network effects, the ability to communicate between systems makes each system that much more valuable. However, it should be noted that many technologies that may be certified by the Commission also may be used to protect content other than Unscreened and Marked Content. Hence, technology licensors should have the right to fulfill their independent obligation to determine which output and recording technologies they wish to approve, so as to ensure the integrity of their respective protection systems for all applications.

8. License Terms

The Commission has stated its view that licensors should license their technologies on a reasonable and nondiscriminatory basis. It is not clear that even this basic requirement is necessary in the context of a list of alternative technologies from which companies may choose – or develop their own technology for use in this context -- but the standard is a common one in many industry settings and not likely as a practical matter to cause worthy technologies to be kept off of the list. In any event, DTLA believes that a technology licensor and marketplace should be free to determine what particular license terms are appropriate to a particular technology. DTLA therefore opposes the suggestion by Philips that the Commission should adopt specific criteria that dictate the terms of technology licenses.

IV. The Technologies, Not The Commission, Should Define The Scope Of The Personal Digital Network Environment.

Paragraph 63. What is the appropriate scope of redistribution that should be prevented. In general, we believe that a flag based system should prevent indiscriminate redistribution of digital broadcast content, however, we do not wish to foreclose use of the Internet to send digital broadcast content where robust security can adequately protect the content and the redistribution is tailored in nature. We see comment on the usefulness of defining a personal digital network environment ("PDNE") within which consumers could freely redistribute digital broadcast television content. If so, we seek comment on the various permutations of a PDNE that were proposed in the BPDG Final Report and whether any modifications are needed to maintain consumer's home viewing expectations. We also seek comment on possible new formulations of a PDNE.

The definition of a PDNE, in the view of DTLA, is effectively coextensive with the goal achieved by a particular protection technology. In general, the goal of redistribution control should be to enable consumers to enjoy Marked Content on devices that the consumer owns, within and outside the home (including an automobile, a vacation home, hotel room, portable digital equipment, etc.). Thus, we agree with the Commission as a general matter that the

regulations should not foreclose use of public networks to facilitate transmission of recorded digital broadcast content for personal uses.

DTLA believes, however, that it is difficult to define a PDNE if viewed as a strict limitation on the capabilities of a particular protection system. It is not possible for technology proponents to state with 100 percent certainty that their technology will prevent, in all circumstances, unauthorized access outside of what one might consider the limits of the home or personal network. A consumer theoretically could drill holes through apartment walls and pass a protected network wire to a neighbor, or could share passwords to a protected home network, and thereby evade technological protections that, in the absence of such intentional misconduct, would suitably limit the scope and use of a PDNE.

For that reason, DTLA has defined in its own licenses the concept of "home and personal network" by reference to the inherent reach of the DTCP technology in the ordinary course of usage, not by other boundaries. From that perspective it may be more appropriate to state what the PDNE includes and what it is intended to exclude, rather than to establish hard and fast borders.

In particular, DTLA believes that functional criteria should not impose any specific limitations, such as an "authorized domain," with which a technology must strictly comply. The attributes of each technology will approximate a home and personal network by function rather than by description, with each technology preventing average consumers from (1) circumventing the protection, and (2) participating in unauthorized internet retransmission of the content. Functional criteria should thus encourage the broadest range of technical possibilities and innovation. DTLA believes that a static "one size fits all" definition of a PDNE could not comprehend the continued innovation of technology and business models -- innovation which should serve as the real basis for defining the network.

V. No Stakeholder Should Be A Gatekeeper.

64. Whether content owners are the appropriate entities to make initial approval determinations, or whether another entity should have decision-making authority. In particular, we seek comment on whether the Commission, a qualified third party, or an independent entity representing various industry and consumer interests should make approval and revocation determinations.

DTLA views the purpose of this proceeding as the protection of the rights of content owners to restrict unauthorized redistribution of digital broadcast content. As such, technologies that have earned the support of content owners should be approved by the Commission. There is no reason to deny certification to a technology that has attained the use or approval of a significant number of content owners, as suggested in the Joint Proposed Criteria.

That said, content owner approval should not be the sole determining factor of which technologies are approved for use. Put another way, content owners can be "gate openers," but must not be "gate keepers." As the Commission rightly observed, no one industry should have the sole discretion to grant or deny technology approval. There must be meaningful alternative methods to obtain certification from an independent entity that has no ties to any specific party with an interest in the outcome. DTLA continues to believe that approval by a government

agency, such as the FCC, would be in best interests of all parties, inasmuch as the Commission will best be able to balance consumer and manufacturer interests against the need to protect copyrighted content.

VI. Rescission of Certifications Should Focus on the Rights of Consumers as Well as Manufacturers and Content Owners, and Should be Prospective Only.

65. As to the issue of how approved content protection and recording technologies may be revoked should their security be compromised, we seek comment on the appropriate standard for revocation. Specifically, we seek comment on whether revocation is appropriate where a content protection or recording technology is perceived to be insecure, or whether the appropriate standard is where security has been compromised in a significant, widespread manner. Once a content protection or recording technology has been revoked, we seek comment on the appropriate mechanism by which revocation should be effectuated. For example, should revoked content protection or recording technologies be eliminated on a going-forward basis, while preserving their functionality for existing devices? We also seek comment on whether there are technological or other means of revoking content protection or recording technologies while preserving the functionality of consumer electronics devices.

DTLA believes that under no circumstances should the Commission require revocation of devices in a case where a protection system has been hacked or otherwise compromised. Revocation of devices, *i.e.*, the intentional disabling of devices already acquired by consumers, would have a devastating impact on consumers whose devices, acquired over a period of years at a cost of billions of dollars, suddenly would be rendered incapable of exchanging content. Such a drastic remedy all but eviscerates the value of equipment in which the consumer has invested. Even the possibility of retroactive revocation of existing devices undermines the willingness to make the necessary investments in the DTV transition and in home networking.

Therefore, any provisions by the Commission affecting the approval of protection technologies should be on a prospective basis only, and should not directly affect the continued use of technologies already within consumer homes.

Thus, rather than "revocation" of a technology, DTLA believes that the focus of inquiry should be upon the circumstances justifying "de-listing" or rescission of a prior Commission certification; in other words, the removal of a content protection technology from a list of approved output or recording protection technologies, such that after a reasonable grace period manufacturers would no longer be permitted to manufacture and sell into the marketplace devices that used a rescinded technology to protect marked content. Even this limited rescission or removal should be viewed as an extraordinary step that could have significant consequences for technology companies and consumers.

The Joint Proposal of the 5C and MPAA Companies had suggested that the criteria for de-listing a technology that has been compromised must be substantially higher than the technology being significantly compromised in relation to its ability to protect Unscreened Content and Marked Content from unauthorized redistribution. That Joint Proposal further recommended that the standard of de-listing a previously-approved technology should take into account the impact on content owners, consumers and manufactures resulting from the continued use of such compromised technology and from any de-listing of such technology.

In further consideration of appropriate "rescission" criteria, DTLA respectfully submits that the Commission should consider the following factors:

a. The level of protection to be maintained by any protection system is that the technology, together with its licensing terms, should be sufficiently robust to "keep honest consumers honest."

b. Any technology can and will likely be hacked; it is more a question of "when" rather than "whether" this will occur.

c. The vast majority of consumers will be completely satisfied with the range of capabilities permitted under the Commission regulations. Consumers candidly are unlikely to dedicate serious efforts to engage in widespread unauthorized redistribution of Marked Content, and have no interest in using or participating in a hack. Yet, rescission decisions affect these law-abiding consumers disproportionately. The Commission therefore should take care not to penalize consumers because of the actions of a small minority.

d. Even where a technology has been hacked, circumvention of the technology may require an affirmative act that is inconvenient, time-intensive, expensive or requires a modicum of skill beyond the reach or interest of the typical consumer.

e. "Enforceability" of a technology does not rely only upon technical robustness. Enforceability for any particular technology combines its inherent technical robustness with the accompanying legal protections provided by license and law. The possibility of legal enforcement can act as a strong deterrent to widespread unlawful conduct. The exercise of legal enforcement can very effectively remedy circumventions and curtail the impact of a technical hack.

f. For these reasons, content protection technologies that have been "compromised" nevertheless remain valuable as part of a comprehensive protection system. Examples: the Macrovision automatic gain control technology could easily be evaded (for many years, lawfully) or unlawfully stripped; yet, it pervasively is used today for protection of analog tapes and analog signals from DVD discs. CSS was circumvented several years ago, and the deCSS unauthorized decryption software remains available; yet, in large measure because of the many factors described above, CSS has retained its value to the motion picture industry, DVD sales continue to skyrocket.

Therefore, DTLA believes that the certification of a technology by the Commission should be rescinded by "de-listing" only on a prospective basis (*i.e.,* for new products) and only if it is clearly and convincingly demonstrated that all of the following conditions are met:

(1) the technology has been so substantially compromised as to be irreparably rendered unable to satisfy the functional criteria established by the Commission,

(2) current use of the means of circumvention of the technology has resulted in actual economic harm to content owners from the unauthorized redistribution of content received by digital terrestrial broadcast,

(3) the means of circumvention of the technology is both capable of use and is likely to be used for unlawful redistribution of Marked Content in a majority of households in the United States,

(4) legal enforcement with respect to the act of circumvention and the means of circumvention are inadequate and,

(5) the demonstrated actual economic harm to content owners from the continued use of the allegedly compromised technology is substantially greater than the harm to consumers from the rescission of approval of the technology.

DTLA thanks the Commission in advance for its consideration of these Comments and the proposals set forth in Appendices A and B hereto, and looks forward to its continued active participation in this proceeding.

Respectfully submitted,

Michael B. Ayers
President
Digital Transmission Licensing Administrator, LLC

Seth D. Greenstein
Chair, DTLA Policy Committee
McDermott, Will & Emery
600 Thirteenth Street NW
Washington, D.C. 20005-3096
(202) 756-8088
sgreenstein@mwe.com